Brief Announcement: Impossibility Results for Optimistic Fair Exchange with Multiple Autonomous Arbiters

Alptekin Küpçü and Anna Lysyanskaya
Brown University, Providence, RI, USA
{kupcu,anna}@cs.brown.edu

ABSTRACT

Fair exchange is one of the most fundamental problems in secure distributed computation. Alice has something that Bob wants, and Bob has something that Alice wants. A fair exchange protocol would guarantee that, even if one of them maliciously deviates from the protocol, either both of them get the desired content, or neither of them do. It is known that no two-party protocol can guarantee fairness in general; therefore the presence of a trusted *arbiter* is necessary. In optimistic fair exchange, the arbiter only gets involved in case of faults, but needs to be trusted. To reduce the trust put in the arbiter, it is natural to consider employing multiple arbiters.

Expensive techniques like byzantine agreement or secure multi-party computation with $\Omega(n^2)$ communication can be applied to distribute arbiters in a non-autonomous way. Efficient protocols can be achieved by keeping the arbiters autonomous (non-communicating). Avoine and Vaudenay [5] employ multiple autonomous arbiters in their optimistic fair exchange protocol which uses global timeout mechanisms; all arbiters have access to loosely synchronized clocks. They left two open questions regarding the use of distributed autonomous arbiters: (1) Can an optimistic fair exchange protocol without timeouts provide fairness when employing multiple autonomous arbiters? (2) Can any other optimistic fair exchange protocol with timeouts achieve better bounds on the number of honest arbiters required? In this paper, we answer both questions negatively. To answer these questions, we define a general class of optimistic fair exchange protocols with multiple arbiters, called "distributed arbiter fair exchange" (DAFE) protocols. Informally, in a DAFE protocol, if a participant fails to send a correctly formed message, the other party must contact some subset of the arbiters and get correctly formed responses from them. The arbiters do not communicate with each other, but only to Alice and Bob. We prove that no DAFE protocol can meaningfully exist.

Categories and Subject Descriptors: F.2.m [Theory of Computation]: Analysis of Algorithms and Problem Complexity - Miscellaneous.

General Terms: Algorithms, security.

Keywords: Optimistic fair exchange, distributed arbiters.

PODC'09, August 10–12, 2009, Calgary, Alberta, Canada.
ACM 978-1-60558-396-9/09/08.

1. INTRODUCTION

Optimistic fair exchange is a very useful primitive in distributed system design with many applications including contract signing, electronic commerce, or even peer-to-peer file sharing [1, 2, 3, 4, 6, 7, 11, 13, 15, 16]. In a fair exchange protocol, Alice and Bob want to exchange some items, and they want to do so fairly. Fairness intuitively refers to Alice getting Bob's item and Bob getting Alice's item at the end of the protocol, or neither of them getting anything, even if one of them maliciously deviates from the protocol. For technical definitions of optimistic fair exchange protocols, we refer the reader to [13].

It has been shown that no general fair exchange protocol can provide complete fairness without a trusted entity [17], called the *arbiter*. In an optimistic fair exchange protocol, the arbiter is not involved unless there is a dispute between the participants. But having a single trusted entity is one of the biggest problems that make the use of such protocols hard in practice. Therefore, the use of multiple arbiters is generally motivated by reducing the trust put on the arbiter [5, 13].[1] A very natural question is how to achieve fairness in the absence of a single trusted arbiter; for example, what if we have n arbiters only a fraction of whom we want to put our trust in? It is clear that this can be achieved using byzantine agreement or secure multi-party computation techniques [12, 8, 9, 10] with $\Omega(n^2)$ communication, but can we do better than that? In particular, can we do anything in a setting where the arbiters need not communicate with each other to resolve disputes?

Avoine and Vaudenay (AV) [5] address this problem in their paper by using verifiable secret sharing techniques to employ multiple arbiters in their fair exchange protocol. They also provide bounds on the number of arbiters that should be honest for their protocol to be fair. A crucial point is that the protocol uses global timeout mechanisms, which assumes all arbiters have access to loosely synchronized clocks, and the arbiters are autonomous (they do not communicate with each other). They leave two important issues as open questions: (1) Can an optimistic fair exchange protocol without timeouts provide fairness when employing multiple autonomous arbiters? (2) Can any other optimistic fair exchange protocol with timeouts achieve better bounds on the number of arbiters that need to be honest?

Unfortunately, in this paper, we answer both of these

[1] It is possible to have multiple arbiters deployed for reducing the load, but if only one of them is employed per exchange, we do not consider that protocol as having distributed arbiters.

questions negatively. Inspired by state-of-the-art optimistic fair exchange protocols with a single arbiter, we define a general class of optimistic fair exchange protocols with multiple arbiters, called "distributed arbiter fair exchange" (DAFE) protocols. Informally, in a DAFE protocol, if one of the participants fails to send a correctly formed message, the other participant must contact some subset of the arbiters and get correctly formed responses from them in order to make the exchange fair. We show that this class of protocols capture currently known state-of-the-art optimistic fair exchange protocols extended to use multiple distributed arbiters in a very intuitive manner. Under this framework, we analyze scenarios that can occur during the execution of instances of optimistic fair exchange protocols, and prove some predicates every such protocol must satisfy to be able to provide semantic fairness, which is a property that needs to be satisfied by all optimistic fair exchange protocols.

2. DEFINITIONS

All the participants (Alice, Bob and the arbiters) are interactive Turing Machines (ITMs)[2]. Those ITMs have the following 4 semantic states: *Working* , *Aborted* , *Resolved* , *Dispute* (see Figure 1).

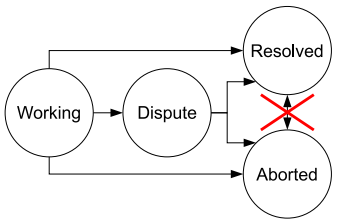

Figure 1: Semantic view of the state machines of the participants.

Distributed Arbiter Fair Exchange (DAFE) protocols: DAFE protocols are optimistic fair exchange protocols that can be characterized with the following:

- Exclusive states assumption
- Connection between arbiters' state and Alice's and Bob's
- Autonomous arbiters assumption

Exclusive states assumption: This assumption states that the *Resolved* and *Aborted* states are mutually exclusive. For an arbiter, those states informally mean whether or not the arbiter helped one of the parties to resolve or abort. We assume that there is no combination of state transitions that can take an honest *arbiter* from the *Aborted* state to the *Resolved* state, or vice versa. In most existing protocols, this corresponds to the fact that the arbiter will not abort with a participant first and then decide to resolve with him or the other participant, or vice versa.

Connection between arbiters' state and Alice's and Bob's: A resolution makes sense if at least one of the parties has not resolved yet. In such a case, Alice or Bob can end in their *Resolved* states (unless they already are in their *Resolved* states) only if a set of arbiters end in their *Resolved* states.

Autonomous arbiters assumption: We assume that the honest arbiters' decisions are made autonomously, without taking into account the decisions of the other arbiters. Arbiters can arrive at the same decision seeing the same input, but they will not consider each other's decision while making their own decisions. In particular, this means no communication takes place between honest arbiters (malicious arbiters can do anything they want).

Semantic Fairness: The semantic fairness property states that at the end of the protocol, Alice and Bob both end at the same state (they both end at their *Aborted* states, or they both end at their *Resolved* states).

Regular DAFE protocols do not have global timeout mechanisms. We show an extended version called DAFE with timeouts (DAFET) where the protocols are allowed to use timeouts. At the timeout specified by the protocol, honest arbiters transition into their *Aborted* states.

3. RESULTS

We prove that no DAFE protocol can provide fairness meaningfully[3], answering the first open question negatively. Even when we extend our framework by relaxing the autonomy assumption about the arbiters, we find out that even broader classes of optimistic fair exchange protocols fall under our impossibility results.

We then switch to the DAFET model to include timeouts. We analyze one existing DAFET protocol [5] using our framework and prove that the previous bounds on the required number of honest arbiters are optimal. No DAFET protocol of the same type can achieve better bounds, since our framework can easily be used to come up with generalized results. See the full paper [14] for details.

4. REFERENCES

[1] N. Asokan, M. Schunter, and M. Waidner. Optimistic protocols for fair exchange. In *ACM CCS*, 1997.

[2] N. Asokan, V. Shoup, and M. Waidner. Optimistic fair exchange of digital signatures. In *EUROCRYPT*, 1998.

[3] N. Asokan, V. Shoup, and M. Waidner. Optimistic fair exchange of digital signatures. *IEEE Selected Areas in Communications*, 18:591–610, 2000.

[4] G. Ateniese. Efficient verifiable encryption (and fair exchange) of digital signatures. In *ACM CCS*, 1999.

[5] G. Avoine and S. Vaudenay. Optimistic fair exchange based on publicly verifiable secret sharing. *ACISP*, 2004.

[6] F. Bao, R. Deng, and W. Mao. Efficient and practical fair exchange protocols with off-line TTP. In *IEEE Security and Privacy*, 1998.

[7] M. Belenkiy, M. Chase, C. Erway, J. Jannotti, A. Küpçü, A. Lysyanskaya, and E. Rachlin. Making p2p accountable without losing privacy. In *ACM WPES*, 2007.

[8] M. Ben-Or, R. Canetti, and O. Goldreich. Asynchronous secure computation. In *STOC*, pages 52–61, 1993.

[9] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC*, pages 1–10, 1988.

[10] R. Canetti and T. Rabin. Fast asynchronous byzantine agreement with optimal resilience. In *STOC*, pages 42–51, 1993.

[11] Y. Dodis, P. Lee, and D. Yum. Optimistic fair exchange in a multi-user setting. *LNCS*, 4450:118, 2007.

[12] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *STOC*, pages 218–229, 1987.

[13] A. Küpçü and A. Lysyanskaya. Usable optimistic fair exchange. In *Cryptology ePrint Archive, Report 2008/431*, 2008.

[14] A. Küpçü and A. Lysyanskaya. Framework for analyzing optimistic fair exchange protocols with distributed arbiters. In *Cryptology ePrint Archive, Report 2009/069*, 2009.

[15] S. Micali. Simultaneous electronic transactions with visible trusted parties. US Patent 5,553,145, 1996.

[16] S. Micali. Simple and fast optimistic protocols for fair electronic exchange. In *PODC*, 2003.

[17] H. Pagnia and F. Gärtner. On the impossibility of fair exchange without a trusted third party. *Darmstadt University of Technology*, TUD-BS-1999-02, 1999.

[2]The ITMs have access to –possibly synchronized– clocks for timeout mechanisms.

[3]Multiple arbiters are no better (or actually worse) than a single arbiter in terms of trust in the DAFE framework.